

FrontEnd Server



FrontEnd Server

FrontEnd Server je řešení určené pro realizaci aplikací, jejichž hlavním rysem je použití mobilního zařízení na straně uživatele jako klientské stanice vzdáleného IS. Výhodou řešení je plně grafického rozhraní na straně klienta a možnost provádět změny v uživatelském rozhraní z centrály bez nutnosti instalace nové aplikace na straně uživatele. Lze využít mobilní telefon, PDA, ale i jiné zařízení (Digitální TV, ATM, PC, PC tablet).

Možnosti použití

- Bankovníctví – služby, nové produkty, marketing
- Sběr dat v energetice a jiných odvětvích
- Dopravní a kurýrní služby
- Informační systémy (jízdni řády, restaurace, kina)
- Herní sázkové systémy
- Nástroje pro obchod s cennými papíry
- Terminál pro CRM, ERP
- Terminál pro technologické procesy

Jak FrontEnd Server pracuje

- Klientská aplikace fungující jako inteligentní aplikační terminál (FrontEnd klient) umí interpretovat vzhled, ovládání a chování aplikace popsané v datových souborech uložených na FrontEnd Serveru v centrále zákazníka
- Data popisující chování aplikace na straně uživatele (grafika, formuláře, taskflow) jsou automaticky stažena do FrontEnd klienta pouze při prvním spuštění nebo při změnách a uložena do paměti klientského zařízení (datový přenos je optimalizován)
- Při práci s aplikací jsou mezi klientským zařízením a serverem přenášena pouze data požádaná uživatelem nebo data pro zobrazení uživateli
- Klientská aplikace spolu spojuje variabilitu tenkých klientů, nízkou komunikační náročnost a rychlost tlustých klientů. Výhodou je snadná změna aplikace bez nutnosti programování na straně klientské aplikace, což je velkým přínosem jak pro IS využívající GPRS spojení, tak pro rozsáhlé pobočkové systémy
- FrontEnd Server slouží pro transformaci dat pro cílový systém a jako úložiště dat popisujících klientskou aplikaci, včetně správy aktivních aplikací

FrontEnd Server

Výhody

- Snadno ovladatelné a přehledné uživatelské rozhraní
- Bezpečná, rychlá a úsporná komunikace (např. GPRS, komprimovaná data, levnější než SIM Toolkit, nebo menší zatížení počítačové sítě v porovnání s klasickým web prohlížečem nebo CITRIXem)
- Nezávislost na konkrétním typu mobilního telefonu (podmínkou je telefon podporující JAVA J2ME MIDP 1.0 nebo vyšší) nebo PC (odstraňuje závislost na verzi OS a JAVA na PC)
- Podpora jiných mobilních zařízení PDA, MDA a dalších „nemobilních zařízení“, jako informační kiosky, bankovní terminály, netPC nebo Digitální Televize
- FrontEnd server může integrovat data a prezentační logiku z více cílových systémů
- Při úpravách aplikace není nutné testování na všech podporovaných mobilních zařízeních
- Na všech zařízeních se aplikace ovládá stejně, náklady a nároky na uživatelskou podporu jsou výrazně nižší
- Oddělení definičních dat od aplikačních snižuje nároky na datové přenosy
- Definovatelná automatická kontrola zadaných údajů na straně mobilní aplikace
- Snadná instalace inteligentního aplikačního terminálu (přes WAP nebo pomocí zprávy MMS)

Podporovaná koncová zařízení

- Mobilní telefony s JAVA J2ME MIDP 1.0/2.0, min. 64KB paměti – Nokia Series 40 a 60, Sony Ericsson, Siemens, Samsung, Alcatel, Motorola, Sharp, LG...
- PDA, MDA a Smartphone s OS PocketPC
- PDA Palm OS
- Inteligentní bankovní terminály
- Informační kiosky s OS Windows
- PC, NET PC

Technologie

FES server: JAVA J2EE, EJB 2.0, aplikační servery BEA WebLogic, IBM WebSphere, Sun Java System Application Server, JBoss, databáze Oracle 9i (volitelně MySQL, PostgreSQL), volitelně platforma MS .NET a MS SQL

FES client: J2ME MIDP 1.0, 2.0 pro zařízení JAVA kompatibilní; J2SE pro zařízení s OS Linux, Windows 2000/XP (PC) MS; .NET Compact Framework pro zařízení s operačním systémem PocketPC 2002, 2003; MS .NET pro zařízení s Windows 2000/XP (PC)

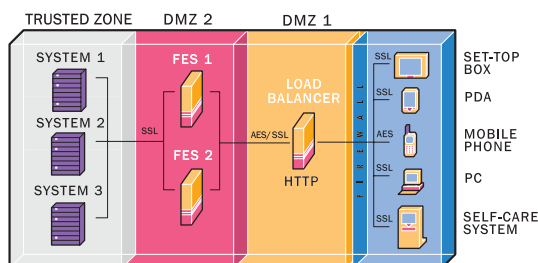
Bezpečnost

- Zabezpečení přístupu k FES serveru – jen autorizovaný klient
- Šifrovaná komunikace 128-256 bit AES mezi FrontEnd Serverem a klientem
- Bezpečný mechanismus výměny šifrovacích klíčů metodou OneTimeKey, kdy nelze ani rozšířením starší komunikace získat šifrovací klíč, ani odvodit nový
- Autorizace dat pomocí digitálního podpisu HMAC zabraňující pozměnění dat
- Zabezpečení výměny hesel pomocí algoritmu OneTimePassword
- Mechanismus předání prvního klíče mimo komunikační cestu
- Veškeré autentizační prvky a šifrovací klíče slouží pouze pro vytvoření bezpečného komunikačního kanálu mezi klientem a FrontEnd Serverem
- FrontEnd Server neobsahuje ani nezaznamenává žádné údaje pro přihlášení do zákaznického systému. Ze serveru tak nelze získat data pro přihlášení k zákaznickému systému
- Pro mobilní zařízení s lepšími parametry procesoru a paměti lze implementovat SSL komunikaci
- V případě nasazení pro PC klientské zařízení je veškeré zabezpečení realizováno pomocí asymetrického šifrování, použití certifikačních autorit

Reference

- Komerční banka – *Mobilní banka KB (květen 2005)*

Schéma řešení



Ukázka aplikace

